PENETRATION TESTING SERVICES

EPI-USE LABS
value through innovation

LEVEL 1: IP-LEVEL

- Open Ports and Services
- Identify Potentially Vulnerable Services
- Unauthenticated Attacks

LEVEL 2: SAP BLACK-BOX TESTING

- Level 1 Plus:
- Identify SAP Specific Avenues of Attack
- Scanning for SAP exposed services
- Identify Potentially Vulnerable SAP Services
- Simulated Outsider Attacks on SAP

LEVEL 3: SAP IN-DEPTH SECURITY TESTING

- Level 2 Plus:
- In Depth SAP Application Layer Testing
- Software Assisted Whitebox Testing for Over 1,000 Attacks
- Identify Insider and Outsider Vulnerabilities

PENETRATION TESTING SERVICES

The three levels of testing cater to the differing expected outcomes and reasons testing is required.

LEVEL 1: This basic test assesses your Internet connected systems as anyone from the outside would see them. We will be able to identify Internet exposed services and in some cases point out specific vulnerable components that could be used to start an attack. The purpose of this test is to identify vulnerabilities that an opportunistic attacker would be able to discover.

LEVEL 2: This is a black-box test, where we do not have any authenticated access to your systems, but would specifically try to compromise the SAP applications. The purpose of this test is to simulate what an outsider attacker would do if they specifically targeted your SAP systems. The limitation of this type of test is that determined attackers can perform reconnaissance and different attack strategies over a long time period, even years. Our services, however, are typically limited to a fixed number of weeks. Therefor it should not be seen as an exhaustive test. Despite these limitations, some organizations require a black-box penetration test for auditing or compliance purposes.

LEVEL 3: This is a white-box test, where we have full access to the systems we test. This allows us to perform software assisted testing for over 1,000 known weakness in total, including 800 SAP-specific tests. Our tests identify weakness in SAP system configuration, access controls, operations and custom code. The test will uncover vulnerabilities that both insiders and outsiders can use to compromise SAP systems.

Disclaimer: The objective of the assessment services are to identify and report on information security vulnerabilities to allow our clients to close the issues in a planned manner, and significantly raising the level of their security protection. However, information security is a continually growing and changing field and testing by EPI-USE Labs does not mean that the a system is secure from every form of attack. There is no such thing as 100% security testing. For example, it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Furthermore, security breaches can, and frequently do, come from internal sources whose access is not a function of system configuration and/or external access security issues.

www.epiuselabs.com | sales@labs.epiuse.com | clientcentral.io

LINKEDIN: EPI-USE Labs | TWITTER : @EPIUSELabs | FACEBOOK: EPI-USE Labs

groupelephant.com™
BEYOND CORPORATE PURPOSE

EPI-USE LABS
value through innovation